

## **II.B. The Primary Tools to Show That the Victim is Not Responsible for the Fraud and to Correct Credit Reports**

Your client should be aware of the two primary tools for an identity theft victim to prove to creditors and other entities where the thief has committed fraud in her name that she is not responsible, and to correct her credit report: the **Identity Theft Affidavit** and the **Identity Theft Report**. Although their names and appearance are similar, these tools provide victims with significantly different rights.

### **A. The Identity Theft Affidavit**

The Identity Theft Affidavit (Affidavit) is the primary tool for proving the victims' innocence to creditors and other entities where the thief has committed fraud in their names. It is a sworn statement that provides critical, detailed information in a comprehensive and standardized manner. It is widely accepted as a means for the victim to dispute fraud committed by the identity thief. Many of the sample dispute letters for consumers' use in [Appendix C](#) of this guide recommend enclosing an Identity Theft Affidavit.

The victim should check with each company where she intends to use the Affidavit as part of her dispute documentation to determine if it accepts the FTC's Identity Theft Affidavit, or if it requires the use of its own proprietary Affidavit.

The Identity Theft Affidavit is available at the FTC's website, at <http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf>, and is at [Appendix D.6](#) of this guide. The victim can either print out a blank copy from the FTC's consumer education website and fill it out by hand, or file an online complaint with the FTC at <https://www.ftccomplaintassistant.gov/>, and print it out with most of the blanks filled in. Whether filling it out by hand or printing it from the FTC's online complaint system, the victim should first gather her information and provide as much detail as possible.

A completed Identity Theft Affidavit provides proof: 1) of the victim's identity; and 2) that she did not commit the frauds alleged in the Affidavit. However, it is understood that the victim may not know, and may have no way to ever determine, many of the facts and circumstances surrounding the crime. The victim should provide as much information as she is able to. A lack of knowledge about, for example, the perpetrator or how the information was stolen, should not be held against the victim or invalidate the Affidavit.

Some companies require that the victim's Affidavit be notarized. Before signing the Affidavit, the victim should find out if the company requires notarization, and if so, wait to sign it in the presence of a notary. The victim should be aware that signing the Affidavit potentially exposes her to criminal penalties for filing false information, since the information may be shared with law enforcement.

For the purpose of disputing a fraudulent account that does not present any complicating factors, the company should not require a police report in addition to the

Affidavit. If no police report is required, your client can leave blank the question regarding law enforcement. If the company does require a police report, your client should inquire as to the reason for the request. If the request seems justified, she should file a police report and fill in the Affidavit's section on law enforcement reports.

When filing the Affidavit with a particular company, the victim should consider redacting information related to accounts with any other companies. The victim should attach copies of her supporting documentation, as proof of her identity and to show that she is a victim of identity theft, and not the person who created the fraudulent accounts or transactions in her name. This would include copies of, for example:

- government-issued identification documents;
- utility bills or other documentation showing the victim's current address;
- a credit report marked-up to indicate which information is inaccurate as a result of identity theft; and
- any bills, collection letters, or other documents related to the fraudulent accounts or transactions.

## **B. The Identity Theft Report**

The Identity Theft Report is the primary tool for removing inaccurate identity theft-related information from the victim's credit report. When the victim provides a qualifying Identity Theft Report and request to a CRA, the CRA under section 605B of the FCRA, is required to block the reporting of information resulting from identity theft from appearing in her credit report within four business days. The CRA also must notify the furnishers of the identity theft-related information (furnishers), who must subsequently cease reporting that information to the CRAs and cease selling the fraudulent debts for collection.

As defined in the FCRA, the Identity Theft Report is a report:

- (A) that alleges an identity theft,
- (B) that is a copy of an official, valid report filed by a consumer with an appropriate Federal, State, or local law enforcement agency, and
- (C) the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information if, in fact, the information in the report is false.

FCRA Section 603(q)(4), 15 U.S.C. 1681a.

Under the authority provided to it by Congress, the FTC modified the definition in several important ways.<sup>1</sup> The FTC's Rule on Related Identity Theft Definitions requires the victim to provide as much specificity as possible, including:

- information about when the loss, theft, or misuse of her personal information occurred,
- any information about the perpetrator,
- the names of companies that furnished the information to the CRAs,
- account numbers for compromised or fraudulently opened accounts, and

---

<sup>1</sup> The FTC's Rule on Related Identity Theft Definitions, 16 C.F.R. Part 603.3, 69 Fed. Reg. 63922 (11/03/04).

- any other information about the theft.

The FTC's Rule also states that a CRA or furnisher may reasonably request additional information or documentation if the Report does not contain enough specificity for it to determine the validity of the alleged identity theft. 16 C.F.R. § 603.3(a)(3). Bear in mind that many identity theft victims do not know – and may never know – who stole or misused their personal information, how it was stolen, or other aspects of the crime. If the victim cannot provide these kinds of details, the police, CRAs, or furnishers should not consider the Identity Theft Report incomplete. For examples of reasonable requests for additional information, see the Commission's Rule on Related Identity Theft Definitions at [Appendix E.12](#). 16 C.F.R. § 603.3(c)(1 - 4).

If the victim has obtained a detailed report from law enforcement, that document could serve as an Identity Theft Report. However, normally, a law enforcement report doesn't contain enough detail to be considered an Identity Theft Report. To help law enforcement develop more detailed reports, the FTC's Identity Theft Affidavit can be used to add detail to a police report. This puts the job of gathering and organizing the information about the crime on the party in the best position to obtain it, the victim.

An Affidavit that has been verified by the police and incorporated into or attached to the police report should contain sufficient detail to avert requests by CRAs or furnishers for additional information.

An Identity Theft Report offers five major benefits to identity theft victims:

- *Blocking fraudulent information from appearing on a credit report:* By submitting an Identity Theft Report to a CRA, a victim can stop the CRAs from reporting information resulting from the identity theft on the victim's credit report. The CRAs have up to four business days after they accept the Report to block the information. FCRA § 605B, 15 U.S.C. § 1681c-2.
- *Preventing a company from refurnishing fraudulent information to a CRA:* Once a CRA informs a furnisher that it has accepted a victim's Identity Theft Report which states that the information the company furnished was caused by identity theft, the furnisher is prohibited from refurnishing that information to a CRA. FCRA § 623(a)(6)(A), 15 U.S.C. § 1681s-2 (a)(6)(A). The same prohibition on refurnishing fraudulent information to a CRA applies if the victim files her Identity Theft Report directly with the furnisher. FCRA § 623(a)(6)(B), 15 U.S.C. § 1681s-2 (a)(6)(B).
- *Preventing a company from selling or placing for collection bad debts that result from identity theft:* Once a CRA informs a furnisher that it has accepted a victim's Identity Theft Report which states that the debts the furnisher reported in the victim's name resulted from identity theft, the furnisher is prohibited from selling those debts to another company for collection. FCRA § 615(f), 15 U.S.C.

§ 1681m(f).

- *Placing an Extended Fraud Alert:* Consumers need an Identity Theft Report to place an extended 7-year fraud alert on their credit reports. FCRA § 605A(b), 15 U.S.C. § 1681c-1 (b). For purposes of obtaining an extended fraud alert, an Identity Theft Report with a simple allegation that identity theft occurred should be sufficient. Thus, victims can use police reports generated through automated systems, such as by telephone or computer, or the victim's Identity Theft Affidavit filed with the FTC. 16 C.F.R. § 603.3(c)(4).
- *Obtaining transaction documents from businesses:* Victims may obtain documents related to fraudulent transactions resulting from identity theft if they submit a police report, an FTC Identity Theft Affidavit (or other affidavit provided by the company), and proper proof of identification to the company where the fraudulent transaction occurred. FCRA § 609(e), 15 U.S.C. § 1681g(e). The statutory construction of section 609(e) is a bit unusual. While section 609(e)'s statutory language specifies a police report and an FTC or company-provided Identity Theft Affidavit, an Identity Theft Report that is comprised of an Identity Theft Affidavit attached to a police report, by definition, meets the section 609(e) requirements.

Police officers who participate in the FTC's nationwide online network of consumer complaints, called "Consumer Sentinel," can add the official police report number along with additional information about the Department to the complaint the victim filed with the FTC, which is stored in the Consumer Sentinel database. The officer can retrieve the victim's complaint from the FTC Consumer Sentinel database by searching for: a) the victim's Social Security number or their FTC Complaint Reference Number, plus b) one of four pieces of their personal information, such as name or phone number. The officer can then print the updated complaint. The police report and department-related information will be printed on the complaint the officer generates for the victim. There are signature blocks for the victim and the officer.

**C. What to do if the victim cannot get a police report or a copy of the police report**

As mentioned in Section I, some jurisdictions may refuse to take police reports from identity theft victims. In other jurisdictions, a police officer may be prohibited from giving the victim a copy of the official police report. If so, the victim may have to explore other options.

*First*, the victim can provide the official with a copy of the "Memorandum to Police on Importance of Taking Police Reports for Identity Theft," contained in [Appendix D.7](#). This document explains why an Identity Theft Report is critical for identity theft victims.

*Second*, the victim can check to see if the law in her state requires police to provide reports for identity theft victims. A map of the states that require the police to take reports from identity theft victims is available at [www.theiacp.org/idsafety/map](http://www.theiacp.org/idsafety/map).

*Third*, the victim can seek to obtain a report from another jurisdiction, such as the jurisdiction where the thief misused her information, or from a different law enforcement agency, such as the state police.

*Fourth*, if the police do take the victim's report, but a) refuse or are unable by law to provide her a copy, or b) are only able to provide her with a basic police report bearing a simple allegation of identity theft, the victim should ask the officer to complete the police report number and department-related information in Question 20, and sign her Identity Theft Affidavit. At a minimum, she should ask for the information to complete Question 20 on her Affidavit. The Affidavit, with the report number and as much information in Question 20 completed as possible, and the basic police report, when available, attached, should satisfy the requirements of an Identity Theft Report.

*Fifth*, if the victim cannot file a report in person, she should inquire about filing an "automated report" over the Internet or telephone. Some jurisdictions only provide identity theft victims automated police reports bearing a simple allegation that an identity theft occurred. Victims who file automated reports are often provided only a written confirmation of filing and a report number, if anything at all. If the victim is using an automated police report to support a request for blocking information from her credit report, the CRA or furnisher could reasonably ask the victim for a completed, notarized Identity Theft Affidavit. To forestall that request, it is suggested that victims write the automated police report number on their Identity Theft Affidavit and attach the automated report confirmation notice (if any). 16 C.F.R. § 603.3(c)(3).

*Sixth*, the victim can ask to file a Miscellaneous Incident Report in lieu of a police report. A Miscellaneous Incident Report is a document created by law enforcement to record non-criminal events or events that require no police action or follow up beyond the initial response. It is a report created for informational purposes only, does not generate a police report number, and is not entered as a crime report into databases used for tracking a department's crime statistics.

*Seventh*, if the victim cannot get any kind of police report from any law enforcement agency using the suggestions listed above, the victim can use her Identity Theft Affidavit filed with the FTC as an Identity Theft Report. In such a case, the victim should check the box under Question 23 indicating that she was unable to file any law enforcement report, and provide the FTC Complaint Number.

**Background Information:** In the Analysis of Comments published with the Final Rule on Related Identity Theft Definitions (69 FR 63927, Nov. 3, 2004), the Commission observed that the fact that some police departments will not take identity theft complaints, combined with the fact that most federal agencies use automated systems to take reports, means that excluding automated reports

generated by federal agencies would unduly burden victims of identity theft. The Final Rule contemplates automated reports generated by the FTC's complaint system as being within the scope of the definition of an Identity Theft Report.

**D. When the victim does not want to file a police report**

There may be reasons a victim chooses not to obtain a police report, even though she cannot get the benefits of an Identity Theft Report without at least attempting to file a police report. Victims who do not want to file a police report cannot provide the CRAs with an Identity Theft Report. These victims should follow the dispute procedures under FCRA section 611, described in [Section III.B.](#)